Enhancing the Security Framework in Cloud Infrastructure

ThamaraiSelviSomasundaram[1], Aparna B Bhat[1],Kannan Govindarajan[1], Kiran S[1]
Madras Institute of Technology, Chennai, India
stselvi@annauniv.edu[1],aps2891@gmail.com[1], kannan.gridlab@gmail.com[1], narutokiran@gmail.com[1]

***Abstract*— In the recent years, cloud computing has emerged as one of the hottest and revolutionizing trends in the field of information technology. Even as more and more people and organizations are migrating towards cloud computing, security issues posed by the cloud is a growing concern.**

In this paper, we propose a layered architecture to enhance the protection of data in cloud infrastructure. The architecture, which is a software solution, mitigates some of the security issues such as DDoS attacks, of data by malicious insiders and hackers and unauthenticated users. It encompasses three layers, the authentication layer, the transport layer and the storage layer. The authentication is done by 'Private cookie authentication scheme' and 'Homomorphic encryption scheme', while the DDOS attacks have been handled by building an analyzer that detects and blocks the attacks. The data is split into different chunks and encrypted before storage. Also an N dimensional mechanism has been proposed for key management, thus ensuring that the interests of the customers at large are protected.

***Index Terms*— Layered architecture, Security issues, DDoS attacks, Packet malformed attacks, Homomorphic encryption, Private Cookie Authentication, Hadoop.**

I. Introduction

According to the NIST, cloud computing is a model for enabling convenient on demand network access to a shared pool of configurable computing resources[1]. Amidst the various benefits offered by cloud computing, security is one of the biggest threats to the growth and use of cloud computing. Hence secure cloud computing is vital for national interests as well as for retaining the belief and the trust of the customers in the organization and in cloud computing.

At the basic level security is provided by the process of authentication. Authentication is the process of proving that someone is whom he/she is assumed to be. There are different methods of authentication such as providing the username and the corresponding password, authentication using devices etc [2] are used. In this paper we propose 'Private Cookie Authentication' [PCA] scheme wherein the concept of cookies is used to strengthen the first of the above mentioned authentication techniques.

DDoS attacks pose a big threat to cloud computing[8].A distributed denial of service attack is a coordinated attack on the availability of services of a given target system or network that is launched indirectly through many compromised computing systems[3][9].The increasing number of distributed denial of service attack must be taken care of to ensure that the legitimate customers are not subjected to any unnecessary discomfort because of the shutting down of server due to these attacks[7]. Basically they are of two types, resource depletion and bandwidth depletion attacks[3]. In this paper we propose the handlingof Flood attacks and Malformed packet attacks. In Flood attack, which comes under bandwidth depletion attacks, the server is flooded with a large number of packets from the attackers. This leads to congestion in the server ultimately leading to its crash. Malformed packet attack, which comes under resource depletion attacks, comes in two flavors, IP address and IP packet options [3]. An analyzer has been designed that detects when the server comes under attack and drops the attacking packets.

The data of the customer is stored in the cloud, the location of which is not known to the customer. The data must be protected from malicious users and malicious insiders who can access the data without the knowledge of the user and the organization. Such concerns can be abated by splitting into chunks, encrypting the data before its storage and using an efficient key management system, guaranteeing the protection from malicious insiders and other malicious users.

II. Proposed Architecture

As the Fig. 1 illustrates, the client has to authenticate himself using the homomorphic encryption system and the private cookie authentication. The packets of an authenticated client then pass through the traffic analyzer.The packets that are found to be legitimate and those which do not pose any threat to the cloud, then enter the cloud.

Finally the data that is stored is encrypted using AES 256 and the key is encrypted using the N times encryption.

III. Authentication Level

We propose the importing of the concept of homomorphic encryption scheme into cloud computing [10].

This is further bolstered by the Private Cookie Authentication (PCA component) which strengthens the traditional password system. In PCA, when the user signs up, a verification key is sent to the user via email or mobile phone. The user is prompted to enter the verification key after the sign up. If the key entered matches the key stored in the database, then a cookie containing the key is set in the user's browser, with a lifetime (t). Every time the user tries to log into the application within the lifetime of the cookie, the key is taken from the cookie and the user need not type in the key. Once the lifetime of the cookie expires and the user tries to login, the process of sending the key to the email or phone

DOI: 03.LSCS.2013.1.63

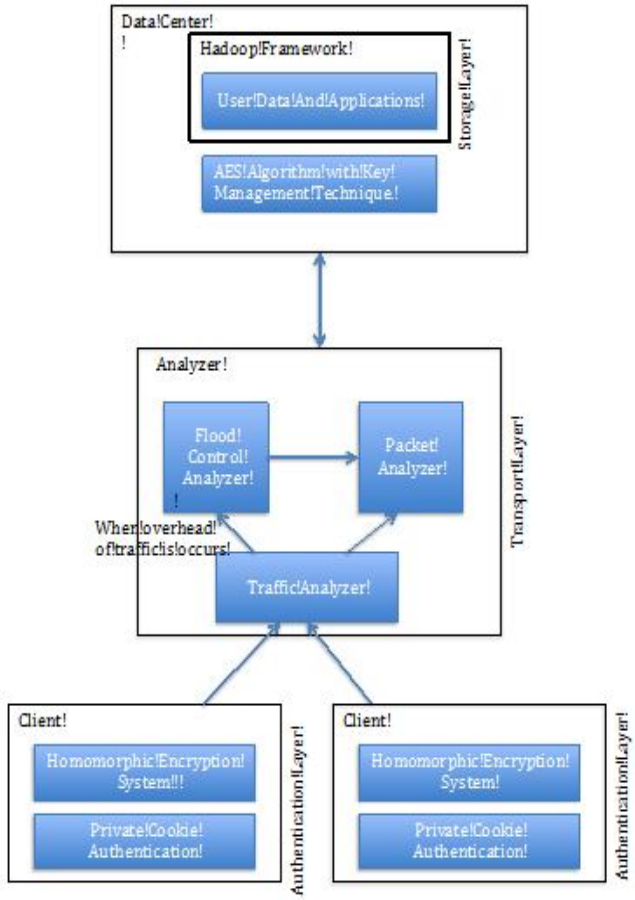

Fig.1.Proposed Architecture

repeats. If the user tries to login from a different browser and the user ID and password match then the key is sent to mail or phone to the legitimate user and the process is repeated.

IV. Transport Level

The analyzer consists of three parts, the Traffic Control Analyzer (TCA), the Flood Control Analyzer (FCA)and the Packet Analyzer (PA).

A. Flood Attack

The TCA captures the packets going through it and keeps a track of the count Ct of the packets received. This Ct is refreshed in every t seconds, where t is a reasonably small value, say 100 seconds. A value called threshold value T is set, which is the maximum number of packets that can be received in**t** seconds. If Ct exceeds T, it indicates that the cloud is probably under attack and the packets are routed to the FCA.

Here, a table I is maintained which contains IP address and the corresponding application level protocol count Ct(ip) each and every IP address, ip.

Here again a threshold value is set for each and every IP called T1. If any Ct(ip) exceeds T1 then the packets belonging to the IP address ip are dropped and the rest are forwarded to the cloud. Thus the attacking packets are removed without causing the congestion it is intended for. If Ct goes below the threshold value, then the packets are routed to the cloud directly without the involvement of the packet analyzer.

C_{thresh}: The threshold value for the total number of incoming packets exceeding which the packets pass through the Flood Control Analyzer (FCA)

I_{thresh}: The threshold for the number of incoming packets per IP Address above which the packets are dropped.

CIP_i : The count of the number of packets per individual IP address. This is maintained inside FCA.

DropList : List of IPs for which the packets are to be dropped

Procedure TRAFFIC CONTROL ANALYZER (Packets,C_{thresh})

Step 1: Capture the incoming packets and maintain Count for every T seconds.
Step 2: If Count exceeds C_{thresh} then
Step 3: Route the packets via the FCA
Step 4: else
Step 5: Clear the contents of the PacketAnalyzer.DropList
Step 6: Goto Step 1.

Procedure FLOOD CONTROL ANALYZER (Packets,I_{thresh},DropList)

Step 1: Maintain count CIP_i for every individual IP Address i.
Step 2: If $CIP_i > I_{thresh}$ then
Step 3: Add the IP Address i to DropList
Step 4: Drop the packets for every IP Address ip present in the DropList

Algorithm 1.DDoS Analyzer

B.Malformed Packet Attack

It comes in two flavors, the IP address attacks and IP packet options attack. In the IP address attack, the source address and the destination address are the same confusing the server and bringing it down. It causes the same packet to go in rounds. The PA component of the DDOS ANALYZER checks if the source and the destination of the packet is same. If so, the packet is dropped.

In the IP packet options attack, all the option fields of the IP packet are set to one. The system spends more time in analyzing the network and hence the productivity suffers. On a greater scale it causes the system to shut down. The PA checks if only one bit in the optional field is set. Failure causes the packet to be dropped.

Thus the DDoS Analyzer detects flood attacks and IP malformed attacks and also takes necessary steps so that the interests of the legitimate users don't come under the scanner.

V. Storage Layer

Before storing the data in the cloud, the data is encrypted to protect the data from malicious insiders and any attackers trying to get their hands on the data. This encryption of data is performed by AES (Advanced Encryption Standard)-256. It is mandatory that the key used for encryption must be kept very safe as it is a symmetric key algorithm.

A. Key Management

For each and every application in the cloud, there is a key

DOI: 03.LSCS.2013.1. 63

box. A randomly generated key is assigned to every customer within the application. This set of randomly generated key is stored in a file. The file is encrypted N times by a Highly Confidential Key (HCK). The HCK and N are with only trusted party and the N times encryption can be carried out only in trusted software. So even if a person gets hold of the key file, he cannot actually make use of it because it is encrypted N times by using AES 256.

Our key management system is based on the concepts of split key management. Like the split key concept, the responsibilities of encryption are split between two keys, the HCK and the key meant for that file.Once the data enters the cloud, if the file is a new file, then a request is sent to the random key generator to obtain a new key. The file is encrypted using AES with the key. Once this is over, the key is encrypted by the HCK N times and is added to the key file. If it's an existing file, the same process is repeated with the key being obtained from the key file and decrypting the key using N and HCK rather than making use of the random generator.For decryption, the key is taken from the key file and decrypted using the HCK and N. The resulting key is then used for decrypting the file.

Hence, the data that is stored in the cloud is always encrypted and hence it guarantees safety from malicious users. The abovementioned key management makes sure that the cipher keys are absolutely safe, thus strengthening the storage layer.

VI. Related Works

PCA component of the authentication layer is inspired by the Google two step verification process [13].Portico's Virtual private data system makes use of split keys and homomorphicencryption to secure the data [4].The Cisco Multi Verification process is designed for protection against DDoS attacks. It works at the hardware level and consists of five layers. These layers analyze the traffic and protect the system against DDoSattacks. Our DDoS ANALYZER work is inspired by this Multi Verification Process but it works at the software level[5].Drop Box and Amazon Web Services Storage gateway encrypt their data using AES 256 before storing it in the cloud thus protecting the data [6].

VII. Results

The Hadoop framework [11][12] was set up in our CARE Laboratory. One System served as the Master node while four systems served as the worker nodes .We deployed our DDOS Analyzer on the machine that served as the master node. For designing and implementing the DDOS Analyzer, we made use of JPCAP.In order to test our analyzer, we first deployed a simple application in the cloud. We used three systems as clients and accessed the application. The number of http packets was around 30 packets for five seconds. We then opened twenty browsers on each of the three systems and opened twenty tabs in each browser amounting to 400 browsers totally. We then made the page refresh automatically every second. We set the threshold to around 100 and the threshold for individual IP to about 30. The results obtained are depicted in fig 2 and fig 3.

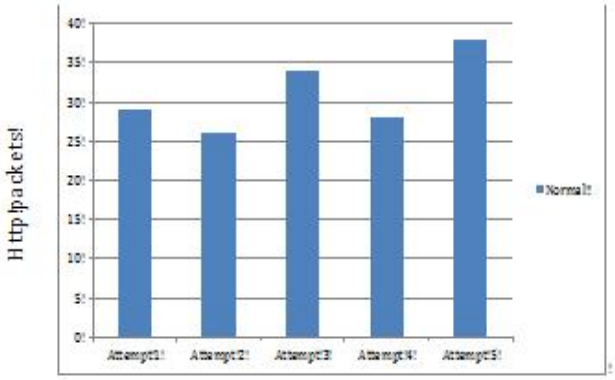

Fig 2. Without DDoS attacks

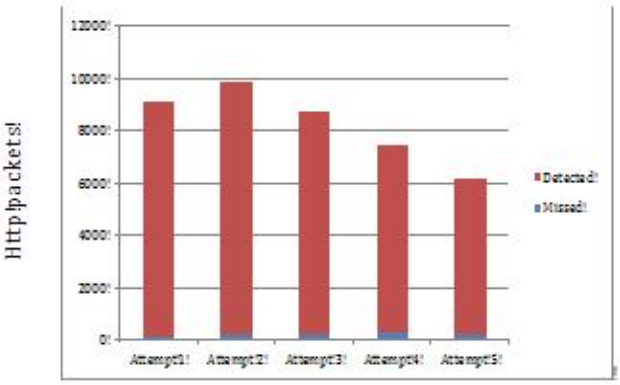

Fig 3. With DDoS attacks

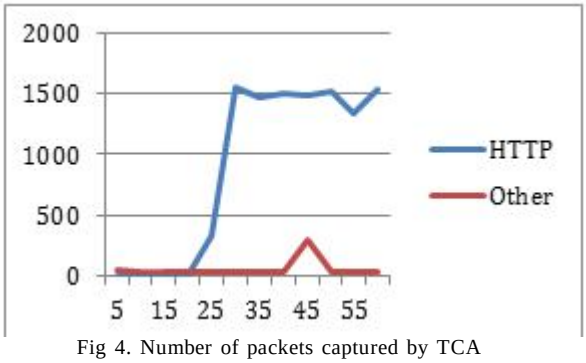

Fig 4. Number of packets captured by TCA

In fig 2, the number of HTTP packets that was captured for every 5 seconds with the help of three clients has been portrayed. Similarly five other attempts have been displayed. In fig 3, the blue colored portion represents the phase during which the attack was not detected while the red colored portion represents the part in which the attack was detected.

In fig 4, the number of packets captured by TCA has been demonstrated. The number of packets captured at intervals of 5 seconds has been shown. The threshold set for the DDOS attack is 1500 and when the number of packets crosses this threshold, the packets are routed to the FCA.

VIII. Futurework

The PCA can further be bolstered by authenticating users based on their MAC address rather than the verification key in the cookie. The DDOS ANALYZER should be made

DOI: 03.LSCS.2013.1.63

scalable, so that it works without any glitch even if there is an increase in traffic. The threshold value should be calculated dynamically based on the expected increase or decrease in the number of users. For example if a new application is launched, the threshold value should be increased. In the key management, the dependency on trusted parties should be removed.

IX. Conclusion

Thus some of the security issues that haunt cloud computing are abated by the layered software solution proposed in this paper. The PCA and homomorphic encryption empowers the authentication provided by the traditional password system. The DDOS analyzer makes sure that the cloud doesn't come under attack from either a flood attack or packet malformed attack. The customer's data is encrypted using AES 256 with the key being further encrypted using the N Times encryption. Hence the customer's data is secured, retaining the trust of the customer in the cloud service.

Reference

[1] Cloud computing, Building a framework for successful transition-CloudWP-8761-C-09, pp 2-4. October 2009.

[2] VinodhaRamanujam and Byron Brasswel, IBM WebSphere V5 Edge of network patterns, IBM, pp 23-25 August 2003.

[3] Stephen M. Specht, Ruby B, "Distributed Denial Of Service: Taxonomies of Attacks, Tools and Countermeasures" Lee-Electrical Engineering,Princeton University. pp 1-4, September 2004.

[4] Securing Data in the Cloud, Meeting the challenges of Data Encryption and key management for business critical applications, Porticor, pp-6, November 2012.

[5] Defeating DDoS attacks, Cisco, pp 7-8, 2004.

[6] Amazon Web Services: Overview of Security Process, pp 13, May 2011.

[7] Dr Lech j.Janczewski, The University ofAuckland, DouglasReamer and JuergenBrendel, JSD Ltd, Auckland, New Zealand, "Handling Distributed Denial-of-Service Attacks", Information Security Technical Report, Vol 6, pp 37-44, No 3. (2001)

[8] Ashley Chonka, Yang Xiang, Wanlei Zhou, "Cloud Security defense to protect cloud against HTTP-DoS and XML-DoS attacks", AlessioBonti–School of Information Technology, Deakin University, Australia,Journal of Network and Computer Application 34 (2011) 1097-1107, pp 1-3, June 2010.

[9] Renaud Bidou, "Denail of Service Attacks", pp3-6, October 2005.

[10] Craig Gentry, "A Fully Homomorphic Encryption Scheme", Department of computer science and the committee on graduate studies of Stanford university, pp 27-31, September 2009.

[11] Mike Olson, "HADOOP: Scalable, Flexible Data Storage andAnalysis**",** Connecting Innovation and Intelligence, Page 14, Vol 1 No.3,2010

[12] AiLingDuan, "Research and Application of Distributed Parallel Search Hadoop Algorithm", International Conference on Systems and Informatics (ICSAI 2012).

[13] Security White Paper: Google Apps Messaging and Collaboration Products, pp 13, May 2011.

DOI: 03.LSCS.2013.1.63